Davis Wright Tremaine LLP

HIPAA 101: HIPAA Privacy for Health Information Exchange

Becky Williams, R.N., J.D.
Partner, Co-Chair, HIT/HIPAA Practice Group
Davis Wright Tremaine LLP
206-628-7769
beckywilliams@dwt.com

Administrative Simplification: What Does HIPAA Do?

- Transaction Standards
- Privacy Standards
  - Restrictions on use and disclosure of PHI
  - Individual rights
  - Administrative requirements
- Security Standards
  - Ensure confidentiality, integrity and availability of electronic PHI
  - Protect against reasonably anticipated:
    - Threats to security or integrity of electronic PHI
    - Uses or disclosures of electronic PHI
  - Ensure compliance by workforce

Affected by HIPAA

- Covered Entities
  - Health care providers engaging in electronic covered transactions
  - Health plans
  - Health care clearinghouses
  - Sponsors of Medicare prescription drug cards
- Other Entities Affected
  - Business Associates
  - Plan Sponsors

Davis Wright Tremaine LLP

Davis Wright Tremaine LLP

General HIPAA Considerations: Preemption

- Is the State law contrary to HIPAA?
- If not contrary, both requirements apply
  - HIPAA preempts or supersedes contrary state law
  - UNLESS state law provides
    - Greater privacy protections
    - Greater individual rights

- Beware participants of multiple states
- Beware "super-confidentiality" information

Davis Wright Tremaine LLP

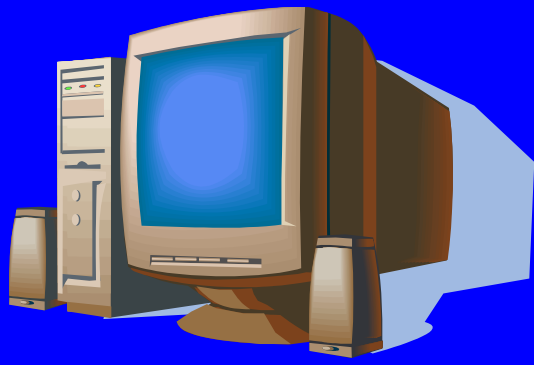
HIPAA Analysis: Take a Pulse

- Identify those with access to PHI
  - Determine covered entity status
  - Determine other status/relationships (e.g., business associate)
- Examine the flow of PHI through HIE
  - Identify who controls the flow of PHI
  - Purposes of the PHI Flow
- Identify relationships and purposes

Davis Wright Tremaine LLP

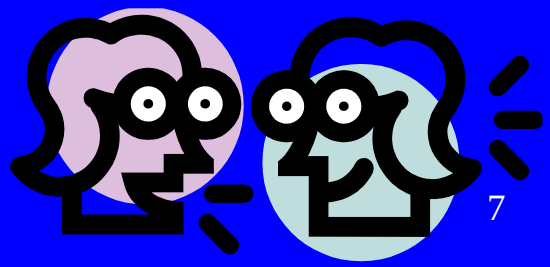
Why is it Important to Take a Pulse

- Separate (e.g., with a master patient index)
  - Leave the decisions to each participant
  - Beware: the degree to which the master patient index constitutes a disclosure
- Centralized but separate (e.g., silos)
  - Holder of EHR likely a business associate
  - BAC plus
  - General rules of disclosures
- Integrated EHR
  - Entries may be a disclosure
  - Probably will want common rules
  - May limit uses and disclosures
  - User agreement



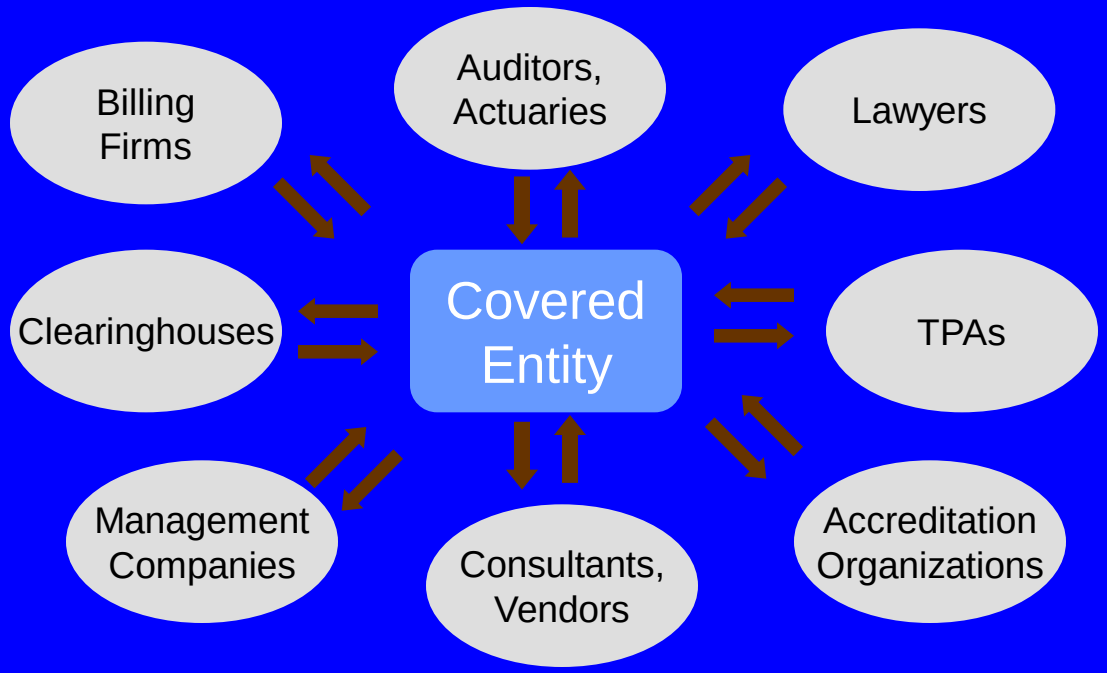
Relationships: Organized Health Care Arrangement

- Medical Staff OHCA
- Community OHCA: organized system
  - More than one covered entity
  - Hold themselves out to the public as a joint arrangement
  - Participate in joint activities that include UR, QA or sharing of financial risk
- May disclose PHI to another covered entity in OHCA for OHCA health care operations in addition to other permitted disclosures
- May use joint notice of privacy practices



Relationships: Business Associate

- A person who, on behalf of a covered entity or OHCA —
  - Performs or assists with a function or activity
    - Involving PHI or
    - Otherwise covered by HIPAA
  - Performs certain identified services

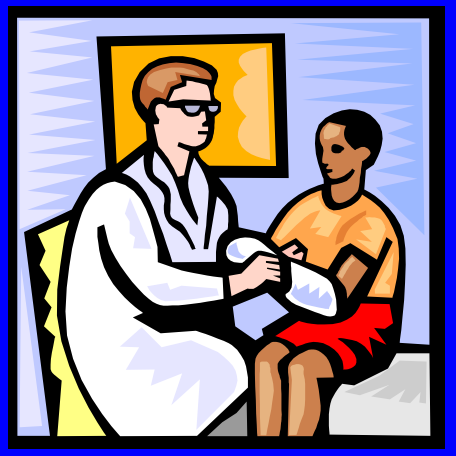


Davis Wright Tremaine LLP

Relationships: Business Associate

- Business associate provides services on behalf of a covered entity involving PHI
  - Examples: management, administration, data aggregation
- Need BAC
- RHIO/ASP/ISP
  - May or may not be covered entity
  - May be a business associate (especially in a hub and spoke arrangement)

PHI Disclosure: TPO



- May disclose PHI for own
  - Treatment
  - Payment
  - Health care operations
- May disclose PHI for treatment activities of a health care provider (not necessarily a CE)
- May disclose PHI to provider or covered entity for recipient's payment purposes
- May disclose PHI to covered entity for recipient's operations
  - For limited operations only (e.g., QA, peer review, fraud and abuse, compliance)
  - If both have/had relationship with patient
  - If disclosure relates to relationship

PHI Disclosure: Authorization

- May not be necessary for most disclosures
  - Depends on participants
  - When in doubt, go with an authorization
- State law may present greatest challenges
  - May be more stringent on disclosures
  - May present problems with authorization
  - Requirements likely to vary with type of info (mental health, AIDS/HIV/STD, developmental disabilities, substance abuse)
- Beware of federal substance abuse requirements
- May want to seek patient permission/ acknowledgement
  - Puts patients on notice; helps to avoid surprises
  - Opportunity to request additional privacy protections
  - Opt in/opt out

Davis Wright Tremaine LLP

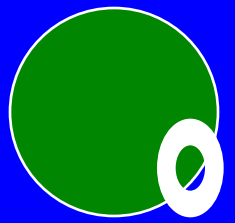
Disclosure: Non-PHI

- De-identified data
  - May be aggregated/shared
  - Is it truly de-identified?
- Limited data sets
  - For public health, research or operations
  - Need data use agreement

Davis Wright Tremaine LLP

Minimum Necessary

- May use, disclose or request only the *minimum necessary* information for the intended purpose
- HIE participants may rely on other members' representation if:
  - All are covered entities and
  - Reliance "is reasonable under the circumstances"
- No minimum necessary for:
  - Treatment
  - Authorization



Individual Rights

- General Issues
  - Need to determine responsibilities
  - Centralized v. de-centralized
- Access
  - If de-centralized, different providers may follow different rules
  - Want to put participants on notice
- Amendment
  - Provider to make determination
  - Process for making amendments system-wide
  - Need to preserve pre-amendment PHI
  - Need to track timing of amendments
  - Need to link to statement of disagreement/ rebuttal

Davis Wright Tremaine LLP

Individual Rights

- Accounting of disclosure
  - Most HIE disclosures not subject to accounting
  - Who tracks?
- Request additional privacy protection
  - Covered entity has right to refuse
  - Accepted request → Bound
  - Practical implication: Who is bound?
  - Be aware of system limitations
- Notice of privacy practices
  - Want all participants to include description of community-wide system
  - Each party is responsible for contents/distribution of NPP
  - Joint NPPs need to be tracked

Davis Wright Tremaine LLP

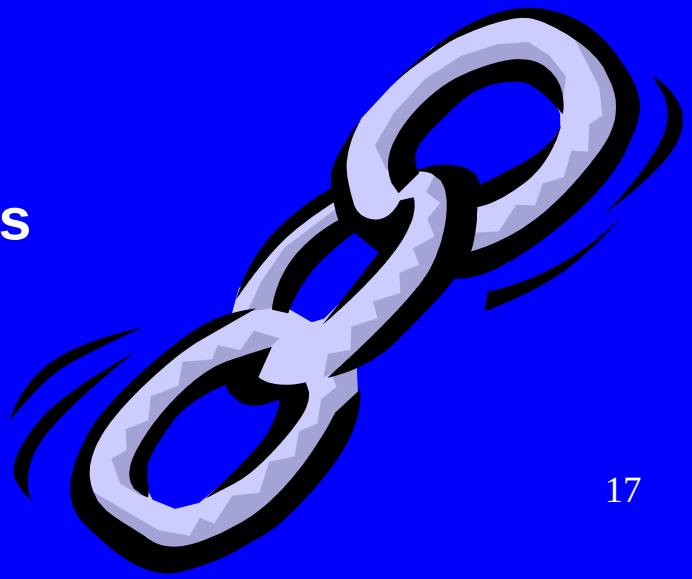
Administrative Responsibilities

- Training
  - Centralized v. decentralized
- Audit/Investigation of complaints
- Mitigation
- Sanctions
  - Each member must have consistent sanctions
  - What about sanctions within HIE (e.g., right to unplug a HIE member)?
- Policies
  - Individual policies and procedures
  - Rules of the road

Davis Wright Tremaine LLP

A Note about Security

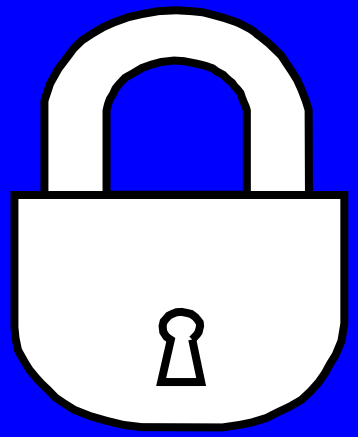
- Security and privacy go hand-in-hand
- Each covered entity is responsible for its own compliance
- Security standards are scalable based on covered entity's sophistication and resources
- Security is only as good as the weakest link
- Should the Health Information Exchange impose minimum requirements?
  - User/license agreements
  - Policies or procedures
  - Membership requirements



Davis Wright Tremaine LLP

A Note about Security

- Again, decision to centralize or decentralize
- Risks vary based on structure
- Ongoing concerns
  - Audit/sanctions
  - Authentication of users
- Systems protections for appropriate access
  - Identify relationship with patient
  - Break the glass



Davis Wright Tremaine LLP

QUESTIONS

?